

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. **(Cancelled)**

15. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an exclusive OR.

16. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation of bit permutation of an intermediate result obtained from execution of an operation of said first chain of operations preceding said operation of bit permutation within said first chain of operations.

17. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation of indexed access to a table.

18. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation which is stable with respect to the application of an exclusive OR function.

19. **(Previously Presented)** The method of claim 34, wherein at least one of said operations in the first chain of operations comprises an operation of transfer of an intermediate result obtained from execution of an operation of said first chain of operations preceding said operation of transfer within said first chain of operations, from one location to another one in a storage space.

20. – 22. (**Cancelled**)

23. (**Currently Amended**) The method of claim 34, wherein the step of randomly choosing comprises generating a random parameter that is used to identify which of said groups of operations to choose, and wherein said method further comprises updating, in parallel with each executed operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

24. (**Currently Amended**) The method of claim 34, wherein further comprising the step of randomly choosing comprises a step of computing a parameter which is equal to a difference between a number of times when an operation of the first chain of operations is one of said groups has been executed during preceding cycles and a number of times when an operation of the second chain of operations is the other of said groups has been executed during said preceding cycles, and when the difference exceeds a given threshold, the step of randomly choosing is conducted so as to decrease decreasing the difference during a current cycle.

25. - 26. (**Cancelled**)

27. (**Currently Amended**) The method of claim 34, wherein the step of storing, at the microcircuit card, the second set of instructions comprises storing instructions for a succession of operations each corresponding to a complement byte by byte of a one of the operations in the first chain of operations.

28. (**Currently Amended**) The method of claim 34, wherein the step of storing, at the microcircuit card, the second set of instructions comprises storing

instructions for a succession of operations each corresponding to a complement bit by bit of a-oneone of the operations in the first chain of operations.

29. (**Previously Presented**) The method of claim 34, wherein the step of storing the second set of instructions for the second chain of operations further comprises a step of applying a permutation of the order of successive commutative operations in the first chain of operations before storing said second set of instructions.

30. (**Previously Presented**) The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. (**Currently Amended**) The method of ~~claim 34~~claim 36, wherein the step of identifying randomly selecting comprises a step of determining the plurality of operations in said third group, said step of determining comprising generating a random parameter before the random selection of the randomly selecting said operations from either the first chain of operations or from the second chain of operations and updating a complementation counter, and the step of outputting the resultant message includes deciding to output the result of the last operation in the uncomplemented state or in the complemented state depending on a state of the complementation counter.

32. (**Currently Amended**) The method of ~~claim 34~~claim 36, wherein the step of randomly selecting identifying comprises a step of determining the plurality of operations in said third group, said step of determining comprising generating a random parameter before randomly selecting said the random selection of the operations from either the first chain of operations or the second chain of

operations and wherein said method further comprises updating, in parallel with each operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

33. (**Previously Presented**) The method of ~~claim 34~~claim 36, wherein the step of identifying comprises a step of determining the plurality of operations in said third group, said step of determining comprising a step of computing a parameter which is equal to a difference between a number of times when an operation of the first chain of operations is executed and a number of times when an operation of the second chain of operations is executed, and when the difference exceeds a given threshold, a next operation to be included in the selected chain of operations in said third group is selected from either the first chain of operations or the second chain of operations so as to decrease this difference.

34 (**Currently amended**) A method of executing and validating a cryptographic protocol between a server entity and a microcircuit card in order to resist a Differential Power Analysis attack against the microcircuit card during execution of said cryptographic protocol, said method comprising the steps of:

storing a first set of instructions for a first chain of operations and a key in both the server entity and the microcircuit card, said first chain of operations forming a ~~data encryption method providing~~ implementing a Data Encryption Standard algorithm,

storing, at the microcircuit card, a second set of instructions for a second chain of operations based on the first chain of operations stored in said microcircuit card, said second chain of operations comprising a succession of

operations each corresponding to a complement of a respective one of the operations in the first chain of operations,

sending a request from said server entity to said microcircuit card for generating a message and sending this said message to the server entity,

executing, at the server entity, when said message from the microcircuit card is received by said server entity, said first set of instructions for the first chain of operations stored therein using said key and said message when received to obtain a server result,

identifying, in the microcircuit card, after reception of the request from the server entity, a selected chain of operations, said step of identifying comprising randomly choosing one of the following groups as said selected chain: 1) all of the operations in said first chain of operations stored in the microcircuit card; or 2) all of the operations in said second chain of operations stored in this microcircuit card as well as an additional complementation instruction;

executing with this said key and this said message which has been sent by, in the said microcircuit card to said server entity in the microcircuit, instructions for the identified and selected chain of operations,

outputting a result of a last operation of the identified and selected chain of operations as a resultant message,

comparing the resultant message to the server result, and

validating the cryptographic protocol between the server entity and the microcircuit card when the server result and the resultant message are identical.

35. (Cancelled)

36. **(Currently Amended)** A method of executing and validating a cryptographic protocol between a server entity and a microcircuit card in order to resist a Differential Power Analysis attack against the microcircuit card during execution of said cryptographic protocol, said method comprising the steps of:

storing a first set of instructions for a first chain of operations and one key in both the server entity and the microcircuit card, said first chain of operations ~~forming a data encryption method providing implement~~ a Data Encryption Standard algorithm,

storing, at the microcircuit card, a second set of instructions for a second chain of operations based on the first chain of operations stored in said microcircuit card, said second chain of operations comprising a succession of operations each corresponding to a complement of a respective one of the operations in the first chain of operations,

sending a message from said server entity to said microcircuit card,
executing, at the server entity, when said message from the
microcircuit card is received by said server entity, said first set of instructions for the first chain of operations stored therein using said one key and said message to obtain a server result,

identifying, in the microcircuit card upon reception by said microcircuit card of the said message coming received from the server entity, a selected chain of operations, said step of identifying comprising randomly selecting for each operation of the first chain of operations in said microcircuit card either said each operation or a respective the corresponding operation in the second chain of operations in said microcircuit card;

executing, in the microcircuit card, instructions for the identified and selected chain of operations using said one key and said message,

outputting a result of a last operation executed in said identified and selected chain of operations either in an uncomplemented state or a complemented state as a resultant message, depending on a number representative of the successive random selections,

comparing the resultant message to the server result, and

validating the cryptographic protocol between the server entity and the microcircuit card when the server result and the resultant message are identical.

37. (**Currently Amended**) The method of claim 36, wherein the step of executing in the microcircuit card further comprises a selection between using the message as itthe message is or using the message in complemented form.